



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/244,203	02/04/1999	BRETT L. HOWARD		3485

7590 08/13/2003

BLAKE CASSELS & GRAYDON LLP  
BOX 25, COMMERCE COURT WEST  
199 BAY STREET  
TORONTO, ONTARIO, M5L 1A9  
CANADA

EXAMINER

CALLAHAN, PAUL E

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 08/13/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/244,203

Applicant(s)

HOWARD ET AL.

Examiner

Paul E. Callahan

Art Unit

2134

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --****Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 27 May 2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 19-30 and 32-35 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 19-25, 28-30 and 32-35 is/are rejected.
- 7) ☐ Claim(s) 7, 26 and 35 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

u

Application/Control Number: 09/244,203

Page 2

Art Unit: 2134

**DETAILED ACTION*****Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5-27-2003 has been entered.

2. Claims 1-18 have been cancelled without prejudice by amendment. New claims 1-19 have been added by the amendment of 5-27-2003 and have been examined.

***Response to Arguments***

4. Applicant's arguments filed 7/11/2002 have been fully considered and when taken together with the changes made to the language of the claims are persuasive to overcome all objections to the amendment to the specification and claims filed 7-11-2003 and overcomes the rejections of the claims under 35 USC 112 first paragraph found noted in the previous Office Action in the case.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Application/Control Number: 09/244,203

Page 9

Art Unit: 2134

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 19, 21, 24, 25, 28, 32, and 34 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Lorenz et al. US Patent 5,799,201.

As per claim 19, 32, and 34; Lorenz teaches a system for ciphering a packet in a data stream received by a communication device (abstract), comprising: a first communications port for receiving said data stream and a second data port for transmitting ciphered data (fig. 2) A memory device having a memory buffer, a first access port receiving bits of data connected to said memory buffer, and a second access port connected to said memory buffer; and a data processing processor connected to said first access port via a first bus; a ciphering processor connected to said second access port via a second bus wherein said first access port and said second access port each provide access to said memory buffer and where data bits making up packets are stored in the memory in a file, (fig.2 items 3a and 3b, items 4 and 5 Data Processors, items 9 and 10 Data Buffers, fig. 3 items 35 Encryptor, col. 4 lines 29-40) said second bus is not connected to said first bus (shown by fig. 2 items 9 and 10 Data Buses not connected) said data processing processor is adapted to receive said data and identify the beginning and end of a packet, and provide said data to said memory buffer over said first bus, said ciphering processor is adapted to receive said data from said memory buffer over said second bus (fig. 2 items 3a, 3b), generate ciphered data from said data, generate integrity check information (col. 3 lines 20-25: autocorrelation and cross correlation functions) for said ciphered data using said data and provide said ciphered data to said memory buffer over said second bus (fig. 3 items 35, 38)

As per claim 21, Lorenz teaches encryption means (fig. 3 item 35 Encryptor) and digesting means for performing verification operations on a packet in a data stream (fig. 1 data processor, fig. 2 items 14, 18 ALU).

Application/Control Number: 09/244,203

Page 4

Art Unit: 2134

As per claim 24, Lorenz teaches a memory buffer that comprises dual port RAM (col. 4 lines 4-10).

As per claims 25 and 28, Lorenz teaches a data processing processor (fig. 2 Data Processor) comprising a security module for retrieving security association data from the memory buffer (fig. 2 items 3a, 3b), for ciphering the data (fig. 3 item 35 Encryptor).

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 20, 22, 23, 29, 30, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lorenz et al. US Patent 5,799,201, and Official Notice taken as detailed below.

As per claims 20, 22, and 23 Lorenz does not teach a hashing means, or a hashing means comprising HMAC hashing means, or an encryption means that uses DES or triple-DES. Official Notice may be taken however, that such steps are old and well known in the art of processor systems utilizing the features of Lorenz and utilized to carry out encryption operations. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated these features into the system of Lorenz. It would be advantageous to do so because use of a hashing means, or a hashing means comprising HMAC hashing, or encryption via DES or triple DES would increase the security of the system.

Art Unit: 2134

As per claims 29 and 30, Lorenz does not teach first and second processors clocked by different clock sources that are asynchronous to one another. However official Notice may be taken that such arrangements of clock sources within processor systems carrying out encryption processing are old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated this feature into the system of Lorenz. It would have been advantageous to do so as this would increase the security of the system by making it more difficult compromise the security of the encryption processing by matching the power consumption of the processors to the encryption processing being carried out.

As per claim 33, Lorenz does not teach the communications system as part of a gateway between a private and a public network in a secure virtual private network. However Official Notice may be taken that the use of such a ciphering system in a gateway or a firewall between a private and a public network is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated the system of Lorenz into a gateway or firewall. It would have been desirable to do so as this would increase the security of data transmitted over an insecure public network.

***Allowable Subject Matter***

9. Claims 26, 27, and 35 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. The following is a statement of reasons for the indication of allowable subject matter: The closest prior art in the field, Lorenz '201, singly and in reasonable combination with the

Art Unit: 2134

other prior art in the field, does not teach the use of security contexts in ciphering operations, stored in a processor and processed in the manner of the claimed invention.

***Conclusion***

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (703) 305-1336.

The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (703) 308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 Official Faxes, (703) 746-7240 Unofficial Faxes, and (703) 746-7238 After Final Faxes.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

8/7/03

*Paul Callahan*